"ALICE"

"BOB"

$\sigma \leftarrow H(x, y, w)$ ~ 102

$s_1, r_1, r_2, r_3, r_4 \overset{R}{\leftarrow} \mathbb{Z}_q$ ~ 104

$E_1 \leftarrow (g^{r_1}, (h_1)^{r_1} x^{s_1})$ ~ 106

$E_2 \leftarrow (g^{r_2}, (h_1)^{r_2} y^{s_1})$ ~ 108

$E_3 \leftarrow (g^{r_3}, (h_1)^{r_3} v^{s_1})$ ~ 110

$E_4 \leftarrow (g^{r_4}, (h_1)^{r_4} x^{-(a_1+c_1\sigma)} y^{-(b_1+d_1\sigma)})$ ~ 112

114 ~ $<E_1, E_2, E_3, E_4, <x, y, w, v>>$

$\Sigma[\Psi, \Gamma]$

116 ~

$\sigma \leftarrow H(x, y, w)$ ~ 118

$s_2, r_5, r'_1, r'_2, r'_3, r'_4 \overset{R}{\leftarrow} \mathbb{Z}_q$ ~ 120

$E_5 \leftarrow (g^{r_5}, (h_1)^{r_5} x^{e_2} (v x^{-(a_2+c_2\sigma)} y^{-(b_2+d_2\sigma)})^{s_2})$
$\times (E_1)^{-(a_2+c_2\sigma)} \times (E_2)^{-(b_2+d_2\sigma)} \times (E_4)^{s_2}$ ~ 124

$E'_1 \leftarrow (g^{r'_1}, (h_2)^{r'_1} x^{s_2})$ ~ 126

$E'_2 \leftarrow (g^{r'_2}, (h_2)^{r'_2} y^{s_2})$ ~ 128

$E'_3 \leftarrow (g^{r'_3}, (h_2)^{r'_3} v^{s_2})$ ~ 130

$E'_4 \leftarrow (g^{r'_4}, (h_2)^{r'_4}) \times (E'_1)^{-(a_2+c_2\sigma)} \times (E'_2)^{-(b_2+d_2\sigma)}$ ~ 132

$<E_5, E'_1, E'_2, E'_3, E'_4>$ ~ 134

$\Sigma[\Psi', \Gamma']$

136 ~

138 ~ $w' \leftarrow x^{e_1} (v x^{-(a_1+c_1\sigma)} y^{-(b_1+d_1\sigma)})^{s_1} \cdot E_5[2] \cdot (E_5[1])^{-\beta_1}$

140 ~ output w/w'

100

FIG. 1

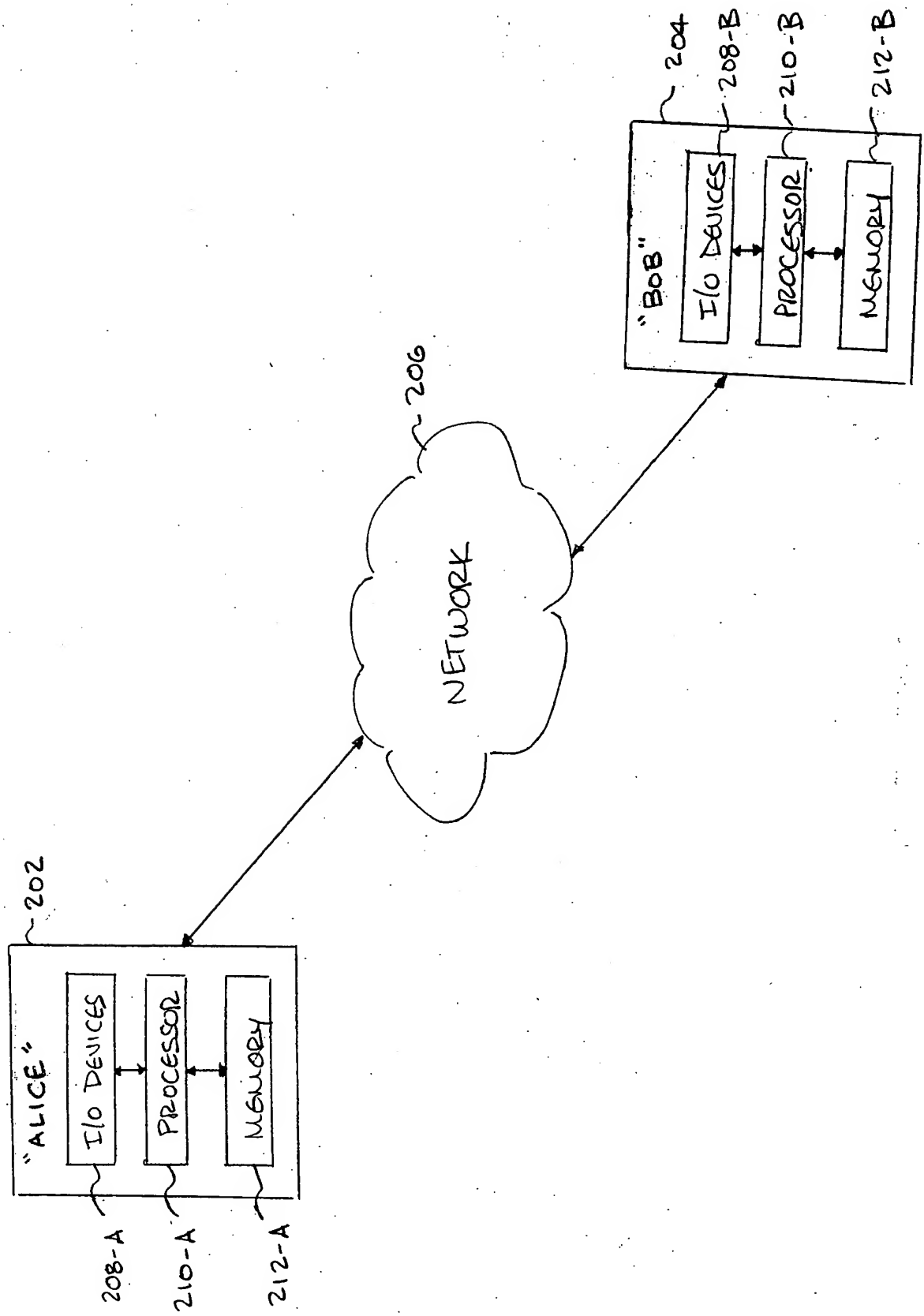
"ALICE"
I/O DEVICES
PROCESSOR
MEMORY
202
208-A
210-A
212-A
NETWORK
206
"BOB"
I/O DEVICES
PROCESSOR
MEMORY
204
208-B
210-B
212-B

FIG. 2